

Amendments to the Claims

1-6. (Canceled)

7. (New) A method of encrypting contents information, comprising the steps of:

generating a first-key signal representative of a first key from first-key base information according to a first function, the first-key base information being a base of the first key;

AI encrypting contents information into encryption-resultant contents information in response to the first-key signal;

generating a second-key signal representative of a second key from second-key base information according to a second function, the second-key base information being a base of the second key;

encrypting at least a portion of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information;

generating transmission-purpose key base information from the second-key base information and an authentication value according to a third function; and

recording the encryption-resultant contents information, the encryption-resultant first-key base information, and the transmission-purpose key base information on a recording medium.

8. (New) A method as recited in claim 7, wherein the first and second functions are one-way functions.

9. (New) A method of encrypting contents information, comprising the steps of:

generating a first-key signal representative of a first key from first-key base information according to a first function, the first-key base information being a base of the first key;

encrypting contents information into encryption-resultant contents information in response to the first-key signal;

generating a second-key signal representative of a second key from second-key base information according to a second function, the second-key base information being a base of the second key;

encrypting at least a portion of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information;

generating transmission-purpose key base information from the second-key base information and an authentication value according to a third function; and

transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, and the transmission-purpose key base information to a transmission line.

10. (New) A method as recited in claim 9, wherein the first and second functions are one-way functions.

11. (New) A method of decrypting contents information, comprising the steps of:

reproducing encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a recording medium;

generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been generated by an encryption-resultant contents information provider side, the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information;

generating second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key;

generating a second-key signal representative of the second key from the generated second-key base information according to a second function;

decrypting the reproduced encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key;

generating a first-key signal representative of the first key from the recovered first-key base information according to a third function; and

decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information.

12. (New) A method as recited in claim 11, wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information.

13. (New) A method as recited in claim 11, wherein the second and third functions are one-way functions.

14. (New) A method of decrypting contents information, comprising the steps of:

receiving encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a transmission line;

generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been generated by an encryption-resultant contents information provider side, the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information;

generating second-key base information from the received transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key;

generating a second-key signal representative of the second key from the generated second-key base information according to a second function;

decrypting the received encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key;

generating a first-key signal representative of the first key from the recovered first-key base information according to a third function; and

decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information.

AI 15. (New) A method as recited in claim 14, wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information.

16. (New) A method as recited in claim 14, wherein the second and third functions are one-way functions.

17. (New) An apparatus for encrypting contents information, comprising:

means for generating a first-key signal representative of a first key from first-key base information according to a first function, the first-key base information being a base of the first key;

means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a second key from second-key base information according to a second function, the second-key base information being a base of the second key;

means for encrypting at least a portion of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information;

means for generating transmission-purpose key base information from the second-key base information and an authentication value according to a third function; and

means for recording the encryption-resultant contents information, the encryption-resultant first-key base information, and the transmission-purpose key base information on a recording medium.

18. (New) An apparatus as recited in claim 17, wherein the first and second functions are one-way functions.

19. (New) An apparatus for encrypting contents information, comprising:

means for generating a first-key signal representative of a first key from first-key base information according to a first function, the first-key base information being a base of the first key;

means for encrypting contents information into encryption-resultant contents information in response to the first-key signal;

means for generating a second-key signal representative of a second key from second-key base information according to a second function, the second-key base information being a base of the second key;

means for encrypting at least a portion of the first-key base information in response to the second-key signal to convert the first-key base information into encryption-resultant first-key base information;

means for generating transmission-purpose key base information from the second-key base information and an authentication value according to a third function; and

means for transmitting the encryption-resultant contents information, the encryption-resultant first-key base information, and the transmission-purpose key base information to a transmission line.

20. (New) An apparatus as recited in claim 19, wherein the first and second functions are one-way functions.

21. (New) An apparatus for decrypting contents information, comprising:

means for reproducing encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a recording medium;

means for generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been generated by an encryption-resultant contents information provider side, the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information;

means for generating second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key;

means for generating a second-key signal representative of the second key from the generated second-key base information according to a second function;

means for decrypting the reproduced encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key;

means for generating a first-key signal representative of the first key from the recovered first-key base information according to a third function; and

means for decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information.

22. (New) An apparatus as recited in claim 21, wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information.

23. (New) An apparatus as recited in claim 21, wherein the second and third functions are one-way functions.

24. (New) An apparatus as recited in claim 21, further comprising means for allowing a user to input the issue ID information.

25. (New) An apparatus for decrypting contents information, comprising:

means for receiving encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a transmission line;

means for generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been generated by an encryption-resultant contents information provider side, the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information;

means for generating second-key base information from the received transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key;

means for generating a second-key signal representative of the second key from the generated second-key base information according to a second function;

means for decrypting the received encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key;

means for generating a first-key signal representative of the first key from the recovered first-key base information according to a third function; and

means for decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information.

26. (New) An apparatus as recited in claim 25, wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information.

27. (New) An apparatus as recited in claim 25, wherein the second and third functions are one-way functions.

A1

28. (New) An apparatus as recited in claim 25, further comprising means for allowing a user to input the issue ID information.
